THEME 8

CRYPTOGRAPHIE

CARRE DE POLYBE _ CHIFFRE DE CESAR

La cryptographie (l'art du cryptage) est une discipline très ancienne utilisée par certains (militaires, scientifiques, … amants) pour protéger ou cacher certains messages souvent à l'aide de secrets ou clés. Lorsqu'un procédé est élaboré, le camp adverse cherche à trouver un moyen de les décrypter. Les Mathématiques ont toujours permis de trouver une solution aux différents cryptages proposés.

CARRE DE POLYBE :

L'historien grec Polybe (205 - 126 avant JC) décrit un moyen de crypter les messages en utilisant un carré (5 x 5) comportant 25 cases (le carré peut comporter 36 cases (6 x 6) lorsque l'alphabet comporte plus de lettres ou lorsque il est nécessaire de coder des chiffres). Notre alphabet possède 26 lettres, le tableau est alors insuffisant pour coder toutes les lettres. C'est pourquoi, le W est éliminé et remplacé par le V ou (dans les pays anglo-saxons principalement) le I et le J sont considérés comme la même lettre.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V W	X	Y	Z

Chaque lettre est alors codée par un nombre formé de deux chiffres : tout d'abord le chiffre de sa ligne suivi du chiffre de sa colonne.

Par exemple, la lettre B sera représentée par 12.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V W	X	Y	Z

Par exemple, pour transmettre un message, Polybe évoque l'utilisation de torches enflammées. Pour envoyer la lettre B, il suffit d'allumer une torche à gauche et deux torches à droites (B correspond à 12)

A Saint-Petersbourg, les prisonniers de certaines prisons utilisaient ce procédé pour communiquer entre eux.

A l'entrée de la prison que l'on peut maintenant visiter, se trouve un panneau représentant un carré de Polybe (un peu plus grand – il y a 28 symboles). Les prisonniers, pour transmettre un message, frappaient sur les murs ou sur la tuyauterie en donnant d'abord le numéro de ligne, puis le numéro de colonne.

Exercice 1 :

a) Quel nombre correspond à la lettre O ?

b) Chiffrez (c'est-à-dire cryptez) le message suivant :

CARRE DE POLYBE

c) Traduisez le message :

25 11 14 35 43 15 32 15 44 33 11 45 23 15 33 11 45 24 42 51 15 44

Nous pouvons également introduire un code secret.

Par exemple le mot **MATH** (pas de lettres apparaissant plusieurs fois dans le mot).

Nous plaçons ce mot dans les premières cases de la grille en décalant les lettres non utilisées. Le carré de Polybe devient donc, avec ce code :

	1	2	3	4	5
1	M	A	T	H	B
2	C	D	E	F	G
3	I	J	K	L	N
4	O	P	Q	R	S
5	U	V	W	X	Y	Z

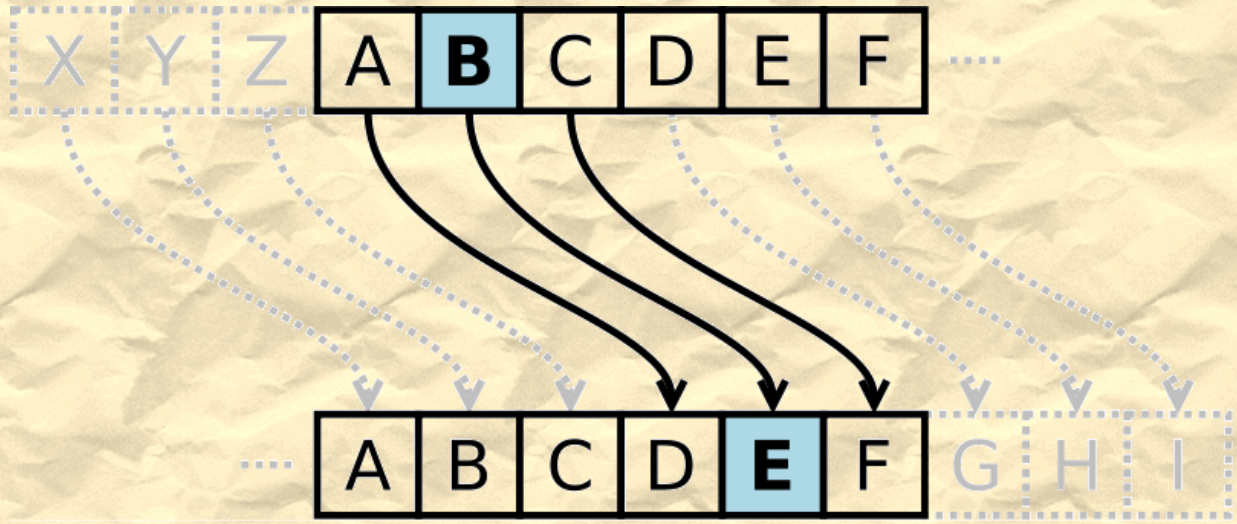
Exercice 2 :

A l'aide du carré ci-contre (carré de Polybe de code MATH), chiffrez (c'est-à-dire cryptez, codez ou brouillez) le message suivant :

CARRE DE POLYBE

CHIFFRE DE CESAR :

C'est un codage simple qui consiste à un décalage (« vers la droite ») des 26 lettres de l'alphabet.
Par exemple, pour un décalage de 3, la lettre A devient D, la lettre B devient E , etc.



Ce codage ne présente que 25 possibilités (l'alphabet comporte 26 lettres, il n'y a donc que 25 façons différentes de crypter un message). Pour casser le code, même en essayant les 25 décalages possibles, il faut peu de temps.
De plus ce type de codage peut être décrypté en utilisant l'analyse des fréquences. En français, le E est la lettre la plus utilisée, suivi du A, puis, selon les textes (texte militaire, texte de la littérature..) du S, du I ,.... Il suffit de repérer dans le texte codé les apparitions les plus fréquentes et de faire un décalage vers la gauche. Plus le texte sera long, plus sera facile cette technique.
Sinon, il est possible d'analyser la fréquence des bigrammes dans un texte, c'est-à-dire la fréquence des groupes de deux lettres (le groupe ES est le plus fréquent, puis LE, suivi de EN, DE , RE …).
Après, l'analyse des trigrammes est possibles(les plus fréquents sont ENT, LES ....)

Exercice 3 :

a) Chiffrez (c'est-à-dire cryptez) le message suivant avec le chiffre de César (décalage 6):

VIVENT LES MATHEMATIQUES

b) Traduisez le message (décalage 6):

IKYZH OKTBU AYGBK FXKAY YO

Remarque : Très souvent, pour compliquer le décodage, les lettres sont regroupées par blocs de 5 , 6 , 4 .... Un mot peut-être à cheval sur plusieurs blocs, et un bloc peut contenir plusieurs mots .

Un peu de Vocabulaire

Le texte initial que nous souhaitons codé s'appelle le texte clair.
Quand il est crypté, le texte est dit chiffré, codé et la méthode s'appelle le code ou le chiffre.
Codé, ce texte s'appelle alors un cryptogramme.
Retrouver le texte clair, c'est décoder, déchiffrer, décrypter ou casser le code.

Le ROT 13 est un cas particulier du chiffre de César (décalage de 13 rangs vers la droite).
L'alphabet comportant 26 lettres, son avantage est que si on applique deux fois de suite le chiffrement, on obtient comme résultat le texte en clair.

Caractère initial	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Caractère chiffré	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Exercice 4 :

a) Chiffrez (c'est-à-dire cryptez) le message suivant avec le chiffre de César (ROT 13):

LES MATHEMATIQUES C EST FACILE

b) Traduisez le message (ROT 13):

YRFZN GURZN GVDHR FPRFG SNPVY R

A SUIVRE